Top Business Continuity and Disaster Recovery Mistakes and

How To Avoid Them

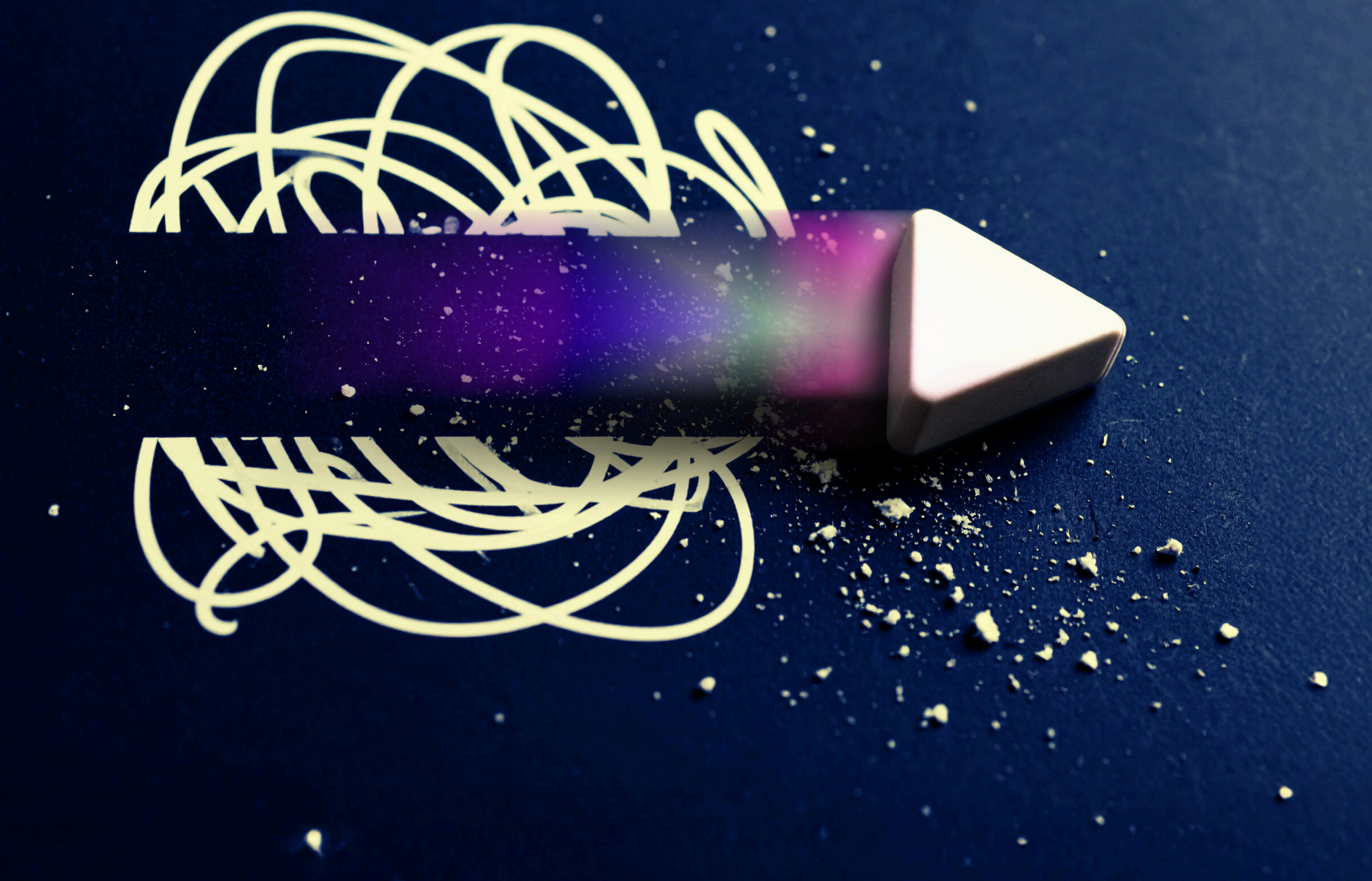


Table of Contents

Introduction

Power outages, cyberattacks, software glitches—disruptions happen. Any one of them can halt your operations, damage your brand and cost you customers.

The good news is you don't need to be an IT expert to start protecting your business. ***What you need is a solid plan.***

A Business Continuity and Disaster Recovery (BCDR) plan helps you stay in control when things go wrong.

Here's what it really means:

- **Business Continuity (BC):**
  Keeps your operations running during and after a disruption.
- **Disaster Recovery (DR):**
  Helps you quickly restore your IT systems, applications and data after a major incident.

In this eBook, we'll walk through the most common BCDR mistakes and how to avoid them. You'll learn how to spot the gaps, avoid costly downtime and implement a practical, tested strategy.

Mistake #1:
Skipping the business impact analysis

The Problem

One of the most common mistakes businesses make is preparing for disruptions without gathering enough facts. You can't dive into disaster planning without first identifying critical functions, dependencies and recovery priorities.

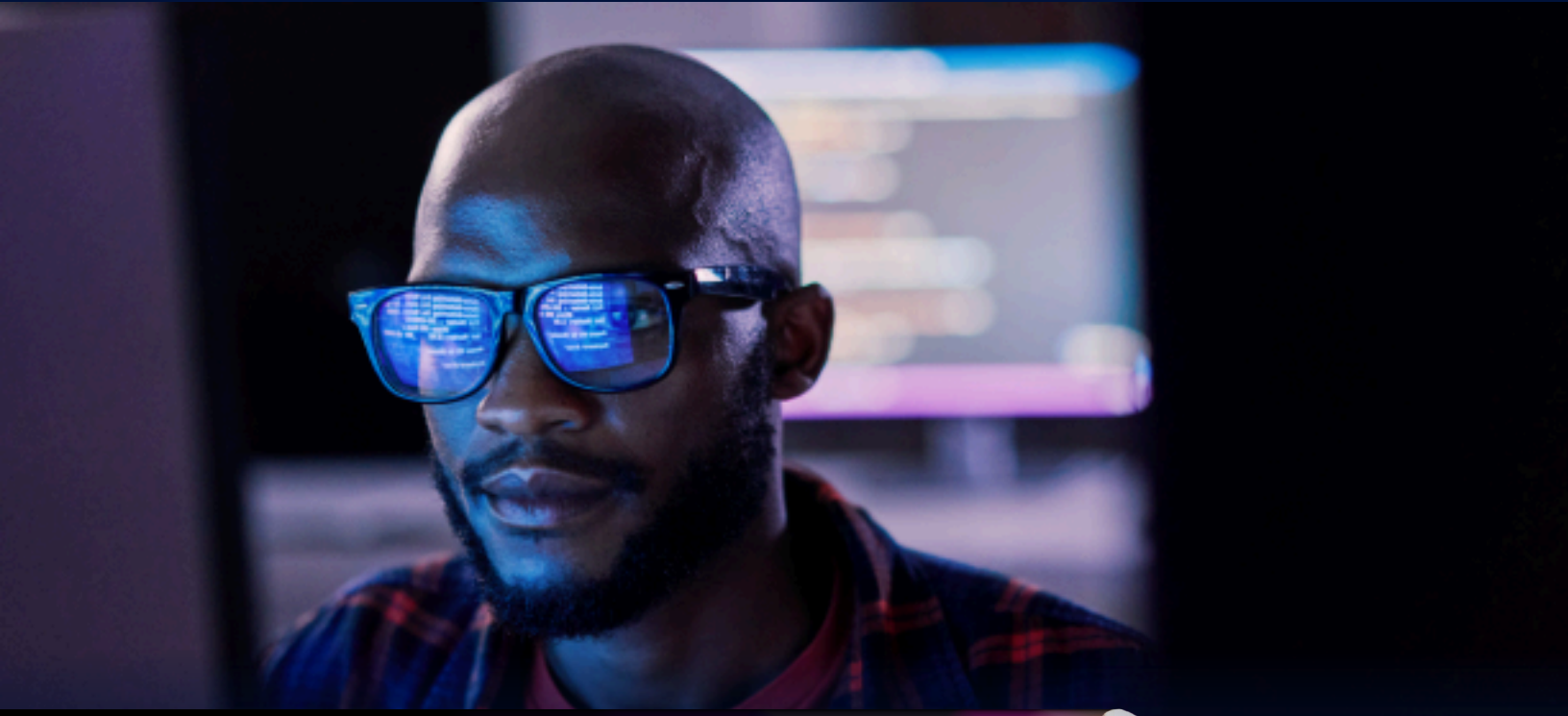
Without a simple business impact analysis (BIA), you're working in the dark. That increases the chances of misaligned priorities, wasted resources and a recovery plan that fails when you need it most.

The Solution

Start by asking the right questions:

- What core business functions must stay operational or be restored quickly?
- What systems, people and processes do these functions depend on?
- What is the financial impact of a disruption?
- How quickly do you need to recover?

A BIA helps you pinpoint what's mission-critical. You'll have a clear view of your priorities so you can design a recovery plan that protects what matters most. This will give you confidence that it will work when things go wrong.



Mistake #2:
Thinking it's just an IT problem

The Problem

While BCDR does involve systems, data and technology, it also involves people, processes and facilities.

By leaving other departments out of the equation, you overlook the broader business impact of a disruption. It's not just about getting back online; it's about maintaining continuity across departments like customer support, HR, finance and marketing.

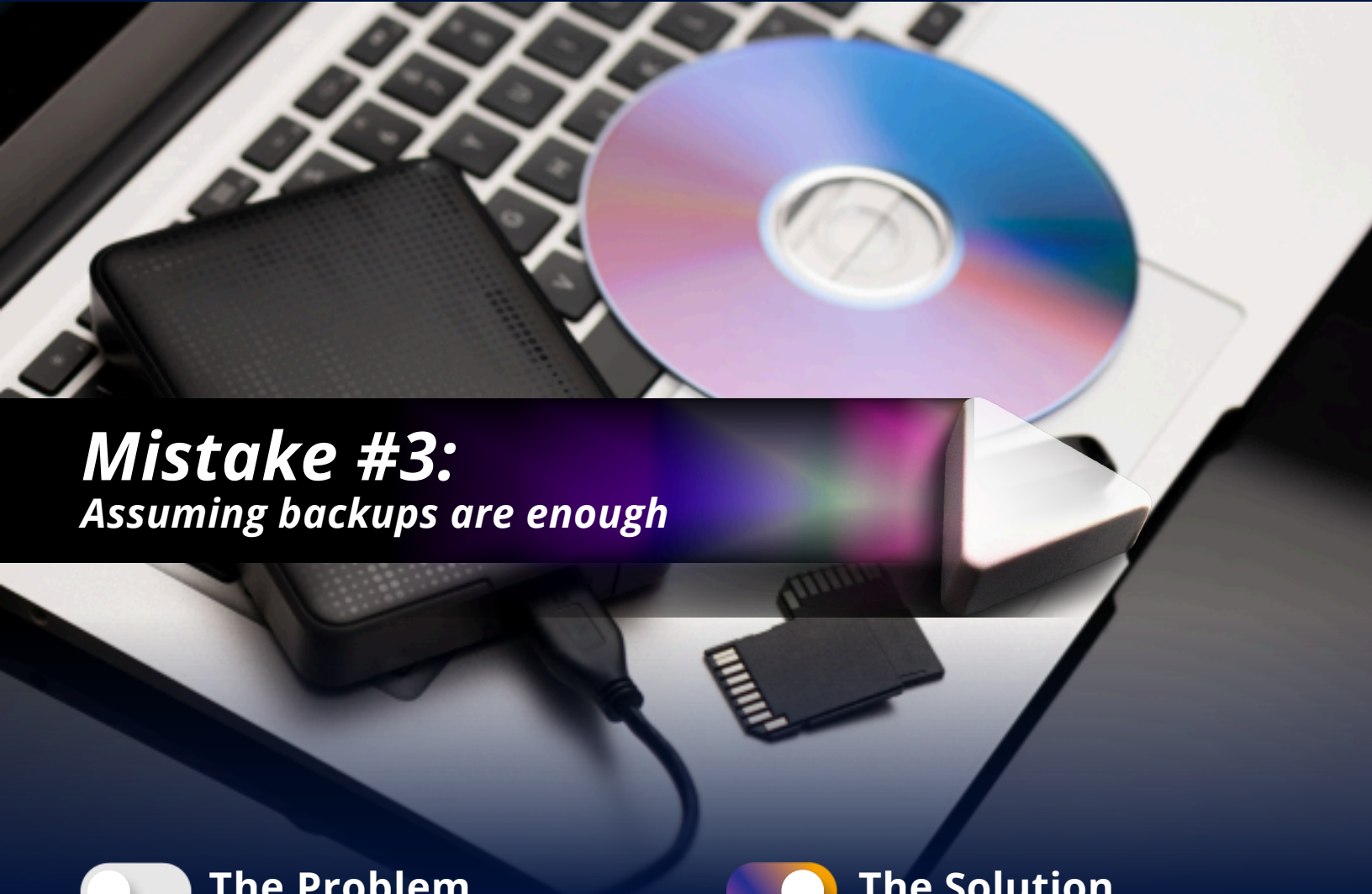
Here's what you risk when BCDR is viewed as only an IT issue:

- Recovery plans that don't align with how the business actually operates
- Confusion around roles and responsibilities during a disruption
- Overlooking interdepartmental dependencies

The Solution

Make it clear that BCDR is everyone's responsibility. Involve leaders from across your organization; include finance, HR, operations and others, and help them understand their role in both response and recovery.

Cross-functional collaboration is critical to designing a resilient continuity plan. Different departments can identify which processes are most essential, what dependencies exist and what resources they need to stay operational during a disruption.



Mistake #3:
Assuming backups are enough

The Problem

Some businesses assume that backing up their data is enough. While backups are a critical component of a disaster recovery plan, they won't keep your business running during a crisis.

Just having a copy of your data doesn't guarantee quick access. There's no certainty that you can restore it to the right systems, and worse, your team might not even know how to access it. In short, even with a backup, you could still face serious downtime.

The Solution

Backups are your safety net, but they're only part of the story. To be truly prepared, you need to understand how your backups support business continuity.

Ask yourself:

- Where are your backups stored, and how do you access them?
- How quickly can you recover your systems?
- Does your team know what steps to follow in an emergency?

A solid recovery plan includes more than just data. It should cover people, processes, locations, systems and timelines. When all these elements are clearly defined, tested and aligned, your backups can truly help you get back to business.

Mistake#4:
Never testing the plan

The Problem

You've invested your valuable time and money into building a BCDR plan. But if you haven't tested your plan, how do you know it will actually work when the time comes?

Often, businesses mistakenly assume that having a plan means they're ready. But when a disaster hits, untested plans can fall apart. During a crisis, clarity is what's needed. There's no time to interpret vague instructions. Your BCDR plan may look great on paper but could have flaws jeopardizing the very future of your business.

The Solution

Run mock tests with the people who would be responsible during a real event. Use these dry runs to look for flaws.

Begin with simple questions such as:

- What happens if your network crashes right now?
- How fast can you switch to the backup?
- Who will communicate with the clients?

These drills help your team execute the BCDR plan with confidence, understand their roles and identify any gaps.

Mistake #5:
Letting the plan become outdated

The Problem

Your business is growing. Teams evolve. You onboard new software and vendors.

But none of these changes have been updated in your existing BCDR plan. If your BCDR plan is outdated, your business is vulnerable when disaster strikes.

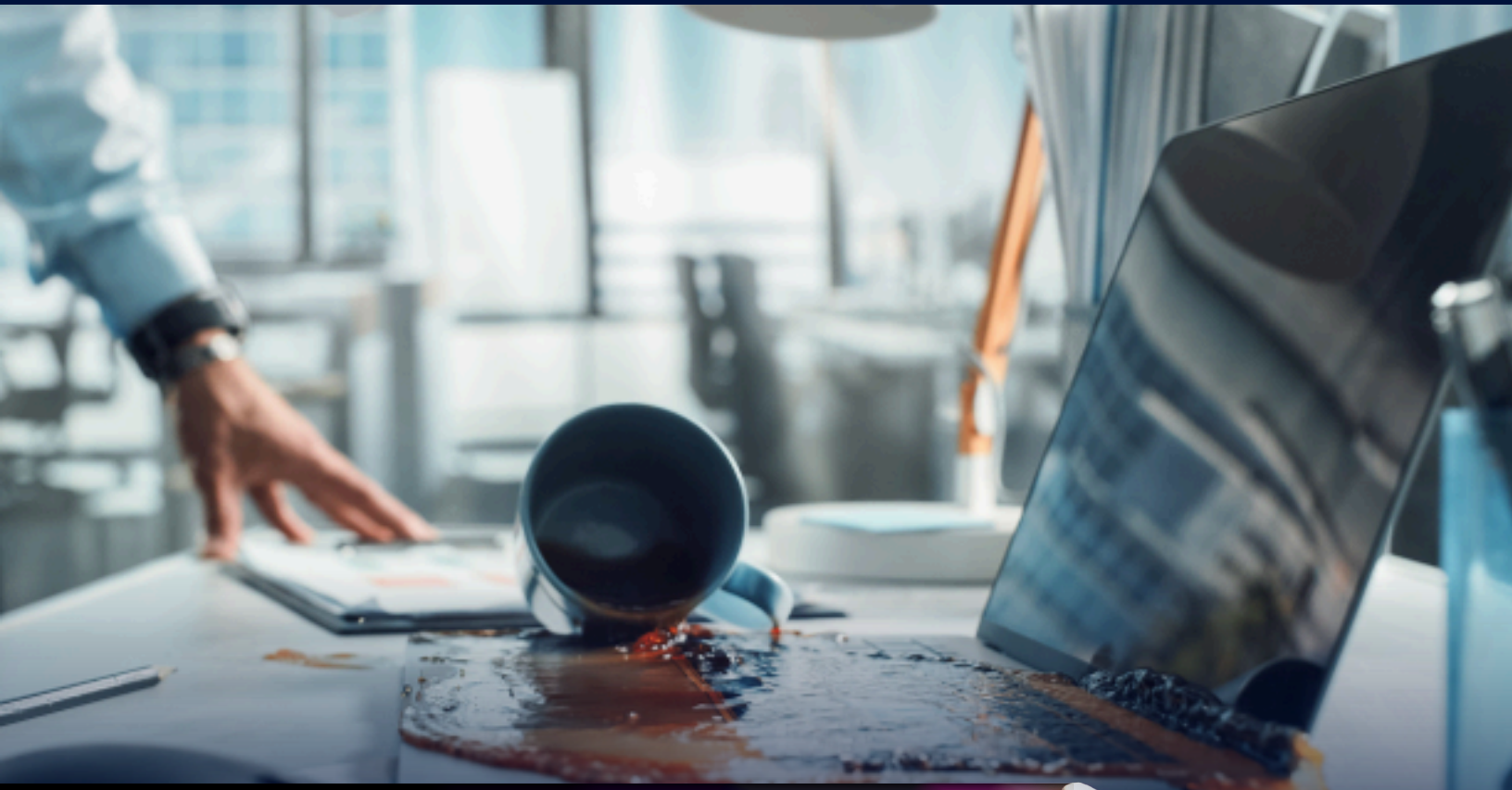
The resulting gaps can slow your response and put operations at greater risk.

The Solution

Here's what an experienced IT service provider will recommend:

- Review your BCDR plan at least once a year.
- Ensure it reflects major changes—new systems, hires or vendors.
- Make sure the plan is easily accessible during a crisis.

If your BCDR plan is current and aligned with your operations, your team will know exactly what to do.



Mistake #6:
Overlooking third-party risks

The Problem

If your business is like most others, your operations rely on third-party vendors. Have you considered the impact your internet provider has on your productivity during an outage? Or if your logistics partner halts shipments due to a natural disaster in their region?

If third-party risks aren't part of your BCDR plan, your plan is incomplete.

Even though the disruption isn't your fault, the fallout still affects you. Customers are unhappy, your business faces downtime and you suffer revenue loss.

The Solution

As the saying goes, "A stitch in time saves nine." Planning for vendor failure now can help you maintain business continuity even when they run into trouble.

Here's where to start:

• Identify your dependencies: Understand how much you rely on each vendor and how that affects your critical operations.

• Check their BCDR plans: Ask whether your vendors have a continuity plan and what happens if they go offline.

• Create workarounds: Build alternatives to keep your business running if a vendor fails.

Mistake #7:
No one knows who's in charge

The Problem

The worst time to ask, "Who's in charge?" is in the middle of a crisis.

Your team should know exactly who leads the response and what each person is responsible for. Without clearly defined roles, confusion sets in, decisions stall and valuable time is lost.

That delay can turn a manageable disruption into extended downtime with serious financial consequences.

Here's how you can bring clarity:

The Solution

A proactive BCDR strategy clearly assigns specific roles and responsibilities.

- Assign a response lead: Designate someone to take charge before an emergency ever happens.
- Clarify responsibilities: Make sure every team member knows who is responsible for what specific tasks.
- Document, share and test: Put it in writing, communicate it clearly and run drills to make sure it works.

Mistake #8:
Communication breakdowns

The Problem

Not knowing how or what to communicate can quickly make a bad situation worse. Often during a disruptive event, no one is sure who should speak, what to say or how to say it.

This confusion only adds to the chaos and impacts employees, customers and vendors alike.

Even the most robust BCDR plan can fall short without a clear and actionable communication plan.

The Solution

How you share information during a crisis shapes how your organization is perceived and how quickly it can recover.

Start with the basics:

- Clarify responsibilities: Decide who sends updates, what they'll say and how messages will be delivered.
- Use multiple channels: Rely on email, phone and text to ensure messages reach people quickly and reliably.
- Prepare templates: Draft prewritten messages to save time when every second counts.
- Assign a lead and a backup: Designate a spokesperson and a secondary contact to maintain continuity.

When done right, clear communication builds trust, reduces confusion and keeps everyone focused on recovery.

Conclusion

Avoiding common mistakes isn't about perfection; it's about preparation. It's about knowing what matters most, involving the right people and having a plan that's tested, current and ready to go.

Resilience isn't luck. It's leadership.

Whether you're building your first BCDR plan or refining an existing one, we can help. Let's build a plan that protects what you've worked so hard to grow.

CONTACT US TODAY

salesteam@fothion.com

(310) 598-7585

fothion.com/contactus